

1 C L A I M S

2 Having thus described my invention, what I claim as new and  
3 desire to secure by Letters Patent is as follows:

4 1. A verification method comprising verifying ownership of  
5 an electronic receipt in a communication system  
6 providing a public key encryption infrastructure,  
7 including the steps of:

8 receiving a message from a sender, said message  
9 being electronically signed by said sender using a  
10 private signature key owned by said sender, said  
11 message includes a receipt which is electronically  
12 signed by an issuer having given said receipt using a  
13 private signature key assigned to said issuer, wherein  
14 said receipt includes details for what said receipt has  
15 been given and a reference to said owner of said  
16 receipt;

17 obtaining a public signature verification key on  
18 the basis of said reference to said owner of said  
19 receipt; and

20 examining whether or not said private signature  
21 key used for electronically signing said message is  
22 associated to said public signature verification key  
23 obtained on the basis of said reference to said owner  
24 of said receipt.

25 2. The method according to claim 1, wherein said reference  
26 to said owner of said receipt is a public signature  
27 verification key associated to a private signature key  
28 held by said owner of said receipt.

1 3. The method according to claim 1, wherein said reference  
2 to said owner of said receipt is a pseudonym used by  
3 said owner of the receipt.

4 4. The method according to claim 3, wherein obtaining said  
5 public signature verification key on the basis of said  
6 pseudonym used by said owner of said receipt includes  
7 getting a certificate securely linking said pseudonym  
8 to said public signature verification key.

9 5. The method according to claim 1, further comprising the  
10 step of authenticating said receipt using a public  
11 signature verification key assigned to said issuer of  
12 said receipt.

13 6. A receipt generation method, comprising generating an  
14 electronic receipt in a communication system providing  
15 a public key encryption system, including the steps of:  
16 receiving a message from a sender, said message is  
17 electronically signed by said sender using a private  
18 signature key owned by said sender, whereby said  
19 message includes a transaction request and a reference  
20 to a designated owner of a receipt to be generated;  
21 authenticating said message using a public  
22 signature verification key associated to said private  
23 signature key held by said sender of said message;  
24 issuing a receipt including said reference to said  
25 designated owner of said receipt and details for what  
26 said receipt has been given; and  
27 electronically signing said receipt with a public  
28 signature key assigned to an issuer issuing said  
29 receipt.

- 1 7. The method according to claim 6, further including the  
2 steps of performing said requested transaction, and  
3 returning said receipt to said sender.
- 4 8. The method according to claim 6, wherein said sender  
5 uses an anonymous communication connection.
- 6 9. The method according to claim 6, wherein said sender  
7 uses a pseudonym for communicating.
- 8 10. The method according to claim 6, wherein said reference  
9 to a designated owner is a pseudonym used by said  
10 designated owner.
- 11 11. The method according to claim 6, wherein said  
12 designated owner of the receipt is the sender.
- 13 12. The method according to claim 6, wherein said reference  
14 to a designated owner is a public signature key  
15 associated to a private signature verification key held  
16 by said designated owner of said receipt.
- 17 13. A method for proving ownership of a receipt, the method  
18 comprising proving ownership of said receipt in a  
19 communication system providing a public key encryption  
20 infrastructure, including the steps of:  
21 creating a first message including a transaction  
22 request and a reference to a designated owner of a  
23 receipt to be generated in response to receiving said  
24 message;

1           electronically signing said message using a first  
2           private signature key;  
3           sending said first message to a first addressee;  
4           and  
5           receiving said receipt from said first addressee,  
6           said receipt being electronically signed by said first  
7           addressee having given said receipt using a private  
8           signature key assigned to said first addressee, wherein  
9           said receipt includes information as for what said  
10          receipt has been issued and said reference to said  
11          designated owner of said receipt.

12   14.   The method according to claim 13, further comprising:  
13          creating a second message including said receipt;  
14          electronically signing said second message using a  
15          second private signature key; and  
16          sending said second message to a second addressee;

17   15.   The method according to claim 13, wherein the first  
18          addressee is identical to the second addressee.

19   16.   The method according to claim 13, wherein the first  
20          private signature key is identical to the second  
21          private signature key.

22   17.   The method according to claim 13, wherein said  
23          reference to said designated owner of said receipt is a  
24          pseudonym used by said owner of the receipt.

25   18.   The method according to claim 13, wherein said  
26          reference to said designated owner of said receipt is a  
27          public signature verification key associated to a

1 private signature key held by said owner of said  
2 receipt.

3 19. The method according to claims 13, wherein said  
4 designated owner of said receipt is identical to a  
5 sender sending said first message to the first  
6 addressee.

7 20. The method according to claim 13, further comprising:  
8 creating a second message including said receipt;  
9 electronically signing said second message using a  
10 second private signature key; and  
11 sending said second message to said designated  
12 owner of said receipt.

13 21. The method according to claim 13, wherein said steps of  
14 sending and receiving of the first message and second  
15 message is performed over an anonymous communication  
16 connection.

17 22. The method according to claim 13, wherein said sending  
18 and receiving of the first message and second message  
19 is performed by using a pseudonym.

20 23. A computer program product stored on a computer usable  
21 medium, comprising computer readable program means for  
22 causing a computer to perform a method according to  
23 claim 1.

24 24. A verification device comprising:

1 means for receiving a message from a sender, said  
2 message is electronically signed by said sender using a  
3 private signature key owned by said sender, said  
4 message includes a receipt which is electronically  
5 signed by an issuer having given said receipt using a  
6 private signature key assigned to said issuer, wherein  
7 said receipt includes details for what said receipt has  
8 been given and a reference to an owner of said receipt;  
9 means for obtaining a public signature  
10 verification key on the basis of said reference to said  
11 owner of said receipt; and  
12 means for examining whether or not said  
13 private signature key used for electronically signing  
14 said message is associated to said public signature  
15 verification key obtained on the basis of said  
16 reference to said owner of said receipt, said device  
17 being for verifying ownership of said receipt in a  
18 communication system providing a public key encryption  
19 infrastructure.

20 25. A receipt generating device comprising:  
21 means for receiving a message from a sender, said  
22 message is electronically signed by said sender using a  
23 private signature key owned by said sender, whereby  
24 said message includes a transaction request and a  
25 reference to a designated owner of a receipt to be  
26 generated;  
27 means for authenticating said message using a  
28 public signature verification key associated to said  
29 private signature key held by said sender of said  
30 message;

1 means for issuing a receipt including said  
2 reference to said designated owner of said receipt and  
3 details for what said receipt has been given; and  
4 means for electronically signing said receipt with  
5 a public signature key assigned to an issuer issuing  
6 said receipt, said device being for generating said  
7 receipt in a communication system providing a public  
8 key encryption system.

9 26. A device for proving ownership of a receipt, said  
10 device comprising:

11 means for creating a first message including a  
12 transaction request and a reference to a designated  
13 owner of the receipt to be generated in response of  
14 receiving said message;

15 means for electronically signing said message  
16 using a first private signature key;

17 means for sending said first message to a first  
18 addressee;

19 means for receiving a receipt from said first  
20 addressee, which is electronically signed by said first  
21 addressee having given said receipt using a private  
22 signature key assigned to said first addressee, wherein  
23 said receipt includes information related to a purpose  
24 for which said receipt has been given, and related to  
25 said reference to said designated owner of said  
26 receipt,

27 said device being for proving ownership of the receipt in a  
28 communication system providing a public key encryption  
29 infrastructure.

- 1 27. A computer program product stored on a computer usable  
2 medium, comprising computer readable program means for  
3 causing a computer to perform a method according to  
4 claim 6.
- 5 28. A computer program product stored on a computer usable  
6 medium, comprising computer readable program means for  
7 causing a computer to perform a method according to  
8 claim 13.
- 9 29. A program storage device readable by machine, tangibly  
10 embodying a program of instructions executable by the  
11 machine to perform method steps for [DESCRIPTION OF  
12 GENERAL FUNCTION], said method steps comprising:
- 13 30. A program storage device readable by machine, tangibly  
14 embodying a program of instructions executable by the  
15 machine to perform method steps for verification, said  
16 method steps comprising the steps of claim 1.
- 17 31. A program storage device readable by machine, tangibly  
18 embodying a program of instructions executable by the  
19 machine to perform method steps for receipt generation,  
20 said method steps comprising the steps of claim 6.
- 21 32. A program storage device readable by machine, tangibly  
22 embodying a program of instructions executable by the  
23 machine to perform method steps for proving ownership  
24 of a receipt, said method steps comprising the steps of  
25 claim 13.



1 33. A computer program product comprising a computer usable  
2 medium having computer readable program code means embodied  
3 therein for causing receipt verification, the computer  
4 readable program code means in said computer program product  
5 comprising computer readable program code means for causing  
6 a computer to effect the functions of the device in claim  
7 24.

8 34. A computer program product comprising a computer usable  
9 medium having computer readable program code means embodied  
10 therein for causing receipt generation, the computer  
11 readable program code means in said computer program product  
12 comprising computer readable program code means for causing  
13 a computer to effect the functions of the device in claim  
14 25.

15 35. A computer program product comprising a computer usable  
16 medium having computer readable program code means embodied  
17 therein for causing proof of receipt ownership, the computer  
18 readable program code means in said computer program product  
19 comprising computer readable program code means for causing  
20 a computer to effect the functions of the device in claim  
21 26.